MANUAL DE CARGOS

Dependencia:	División Control Operativo	**Área**	Área Seguridad Operativa Informática
Código del Cargo:	3010	**Código del Puesto:**	3010
Categoría	20	**Nombre del Puesto:**	Profesional PED 1
Nombre del Cargo:	Ingeniero Gestión Operativa Seguridad Informática - Junior	**Reporta a:**	Jefe Área Seguridad Operativa Informática
Objetivo del Cargo:	Profesional encargado de la ejecución de la seguridad informática, en cuanto a la implementación y mejora institucional, contribuyendo así con la disminución del riesgo para la entidad y asegurando la continuidad del negocio, participar en la organización de la arquitectura de los sistemas informáticos y la definición de controles y procedimientos sobre seguridad de la información, la gestión de análisis de estado de los sistemas, equipos informáticos y tendencias sobre los sistemas de seguridad informática.		

Volver a indice

MACRO PROCESO	PROCESO	ACTIVIDAD		FUNCIONES PRINCIPALES
			1	Controlar y dar seguimiento a la aplicación de los procedimientos relacionados con sus actividades.
			2	Acatar y velar por el cumplimiento constante de políticas, normativas, reglamentos y procedimientos relacionados a la seguridad informática.
			3	Elaborar y llevar el control de las bitácoras de eventos, cronogramas de trabajo, minutas de las reuniones a las que asiste, estadísticas, así como los informes que requieran las labores del puesto.
			4	Confeccionar y presentar informes diversos sobre las actividades realizadas y hacer las recomendaciones pertinentes.
			5	Participar en reuniones con la Jefatura para la asignación de prioridades de tareas o proyectos.
			6	Identificar mejoras en aspectos de procedimientos o normativas.
			7	Participar en proyectos informáticos cuando le sea solicitado.
			8	Investigar, crear, proponer y difundir nuevas formas de trabajo y herramientas para la automatización y gestión de los recursos informáticos propios de la dependencia.
			9	Ejecutar otras tareas propias del puesto.
				FUNCIONES ESPECÍFICAS
			10	Participar en equipos de trabajo para el desarrollo de las funciones propias de la dependencia, así como en proyectos de carácter institucional y de monitoreo de la seguridad de la información.
			11	Tomar en consideración los análisis de tendencias en materia de seguridad información y tecnologías emergentes, así como la información sobre posibles y nuevas amenazas, con el fin de ajustar los controles correspondientes o bien recomendar mejoras en cuanto a controles para mitigar incidentes de seguridad de la información.
			12	Implementar y actualizar los controles que permitan el cumplimiento de las regulaciones, normativas, políticas, procedimientos, buenas prácticas con respecto a los procesos de seguridad informática; de forma tal, que coadyuven en la consecución de controles para la disponibilidad, confidencialidad e integridad de la información y sus tecnologías.
			13	Mantener en un nivel aceptable de riesgo de seguridad de la información de acuerdo con la política de seguridad o normativa relacionada.
			14	Facilitar la información necesaria para el análisis, definición e identificación de la arquitectura tecnológica de seguridad informática requerida en el Conglomerado.
			15	Operar los controles preventivos y de detección de software malicioso (virus, gusanos, software espía y correo basura).
			16	Participar en la definición de la organización de la seguridad lógica y física de la plataforma tecnológica del Banco.
			17	Operar las herramientas que permitan mantener un adecuado nivel de seguridad en la infraestructura tecnológica de la Institución.
			18	Participar en procesos de gestión de Riesgo de Seguridad Informática, recomendando e implementando planes de acción para su mitigación.
			19	Contribuir con la elaboración del Plan de Seguridad de TI, considerando los requerimientos del negocio, la configuración de TI, los planes de acción del riesgo de la información.
			20	Aplicar controles de seguridad de la información para el resguardo de activos sensitivos y de la tecnología de seguridad.
			21	Aplicar controles de seguridad y procedimientos de gestión que permitan la transmisión de datos en la red de forma segura.
			22	Ejecutar las medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
			23	Actualizar controles de seguridad y procedimientos de gestión que permitan el aseguramiento de los dispositivos de usuario final.
			24	Ejecutar los mecanismos para asegurar los derechos de acceso de los usuarios, de acuerdo con los requerimientos de las funciones y procesos de negocio.
			25	Llevar a cabo los planes de pruebas periódicas de la seguridad del sistema (software base, sistema operativo, base de datos y demás componentes) y realizar pruebas de intrusión periódicas para determinar el estado de protección de los sistemas y la red.
			26	Identificar amenazas y vulnerabilidades sobre los activos y procesos de TI, (infraestructura, base datos, aplicaciones, entre otros).
			27	Administrar sistemas criptográficos de TI, de acuerdo a las políticas y procedimientos establecidos, que ayuden a asegurar el ciclo de vida de los certificados digitales (generación, cambio, revocación, destrucción, distribución, almacenaje, uso, modificación y acceso desautorizado).
			28	Apoyar cuando sea requerido en la definición y ejecución de los planes de acción de continuidad de TI.
			29	Atender incidentes y reportes de seguridad informática (administrar los problemas, analizar la causa raíz, identificar, registrar y analizar soluciones de los mismos).
			30	Gestionar solicitudes de servicio (aplicativos).
			31	Ejecutar en conjunto con los proveedores los planes de trabajo para la ejecución del mantenimiento y soporte de las plataformas de seguridad cuando sea requerido.
			32	Apoyar en la capacitación a los usuarios en materia de seguridad informática.
			33	Efectuar Auditorías de Seguridad Informática en procesos, productos y actividades de la Dependencia, evaluando el riesgo en cuanto a seguridad de la información, la factibilidad técnica de los proyectos informáticos y emitiendo recomendaciones de seguridad.
			34	Apoyar la implementación y actualización de las herramientas que conforman la arquitectura tecnológica de seguridad informática tanto de hardware como software.
			35	Ejecutar respaldos periódicos de las bases de datos y configuraciones de la infraestructura tecnológica de seguridad.
			36	Verificar que todos los usuarios (interno, externo y temporal) y su actividad en los sistemas de TI (uso de negocio, operación de sistema, desarrollo y mantenimiento) tengan una única identificación.
			37	Revisar que los derechos de acceso de usuario a los sistemas y a los datos estén de acuerdo a las necesidades del negocio y a los requisitos de trabajo.
			38	Asegurar que las técnicas y los procedimientos relacionados con la seguridad (firewalls, aplicaciones de la seguridad, segmentación de la red y detección de la seguridad de la intrusión) son usados para acceso autorizado desde y hacia la red.
			39	Participar en la implementación del control interno, seguridad y auditoría durante la configuración, la integración y el mantenimiento del hardware y del software para proteger los recursos, asegurar su disponibilidad e integridad.
				FUNCIONES RELACIONADAS CON RIESGO
			40	Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			41	Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			42	Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			43	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			44	Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			45	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.

			46	Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			47	En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
			FUNCIONES RELACIONADAS CON SUGEF	
			48	Según el Acuerdo SUGEF 14-17 "Reglamento General de Gestión de la Tecnología de Información", el cual establece los requerimientos mínimos para la gestión de tecnología de información que deben de acatar las entidades supervisadas y reguladas del sistema financiero costarricense y en concordancia con la Ley de Control Interno, Capítulo III, Sección I "Deberes del jerarca y los titulares subordinados", capítulo 12,13 y 14, este puesto es responsable del desarrollo de las actividades y tareas que le asignen velando por un adecuado ejercicio del mismo, debe garantizar la eficiencia y eficacia de las operaciones que le corresponde ejecutar tomando las medidas correctivas en beneficio de la institución. Por el nivel del puesto deberá promover mecanismos y procesos que mejoren el sistema de control interno en la gestión que le corresponde realizar. Debe procurar mantener las operaciones con un nivel de riesgo aceptable.

CODIGO	REQUISITOS EXIGIBLES	
	Formación Académica:	Bachillerato en Ingeniería de Sistemas u otra carrera afín relacionada con las funciones del puesto.
	Legales:	No aplica.
	Experiencia:	Dos años de experiencia en actividades propias a las descritas.
CODIGO	*** REQUISITOS TÉCNICOS EXIGIBLES**	
	Contar al menos con una especialización certificada y vigente en materia de seguridad de la información, tales como:	
	1. Certified Ethical Hacker (CEH)	
	2. Certified Information Security Manager (CISM)	
	3. Certified Information Systems Security Professional (CISSP)	
	4. Certified CompTIA Security+	
	5. CSX Practitioner	
*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.**		
CODIGO	**REQUISITOS TÉCNICOS DESEABLES**	
	1. Conocimiento de las leyes aplicables al Conglomerado de normativa interna, reglamentos, directrices y circulares que regulan la actividad del Conglomerado.	
	2. Conocimiento en Inglés Técnico (comprensión y lectura).	
	3. Conocimiento en Operaciones de Seguridad de la Información y Gestión de Incidentes.	
	4. Conocimiento en Gestión de riesgo, brechas y el Modelado de amenazas de Seguridad de la información.	
	5. Conocimiento de Seguridad en Telecomunicaciones, Sistemas Operativos (al menos en versiones recientes Microsoft Windows) y Base de Datos (al menos en versiones	
	6. Conocimiento en Control de Acceso y Gestión de Identidades físicas y lógicas.	
	7. Conocimiento en Ejecución y Análisis de pruebas de seguridad.	
	8. Conocimiento en Administración de Infraestructura de Llaves Públicas.	
	9. Conocimiento en los estándares ISO 27000.	
	10. Conocimiento en el estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS).	
	11. Conocimiento en la Ley de delitos informáticos y norma SUGEF 14-09.	
	12. Redacción de Informes Técnicos.	
CODIGO	**SISTEMAS UTILIZADOS**	

COMPETENCIAS REQUERIDAS					
PERFIL KOMPE DISC:		**PERFIL: PROFESIONALES SOPORTE**			
CODIGO	**Cardinales**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CODIGO	**Gerenciales**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CODIGO	**Negocio**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CODIGO	**Soporte**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CODIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Este perfil se aprueba con oficio GGC-1028-2018 de la Gerencia General Corporativa (Acta DGCA-Act.08-2018 (División Gestión de Calidad). Se incluyen Funciones de Riesgo las cuales se incorporan a los perfiles con la aprobación de la Gerencia General Corporativa, emitida en el HT-493-GGC-2019, de fecha el 14 de octubre 2019. Referencia: DIRGE-689-2019 / DIRCH-1477-2019.**				

MSc. Mauricio Durán Ross
Jefe, División Cultura y Desarrollo

Ing. John Richard Molina Nuñez
Director, Dirección Tecnología de la Información